5Gのセキュリティ：
求められるソフトウェア・イノベーションの活用

5Gネットワークにはビジネスと個人の生き方を変える大きな可能性があり、世界各国の政府が5G技術の開発と展開にしのぎを削っています。5Gネットワークは広範な新しい利用を可能にする速度の飛躍的進歩、遅延の低減、そしてフレキシビリティをもたらします。とりわけ5Gは、2023年までに「機器数が2000億」を超えると予想される、モノのインターネット（IoT）の膨大な拡張を支える役割を果たすでしょう。そしてこうした技術は世界経済を根本から変え、数十億人の生活の質を向上させるとともに、デジタルエコシステムを作り変え、人間の現実世界との関わり合い方に変化をもたらすでしょう。

クラウドサービスは5Gにとって今後非常に重要となるため、5Gは多くの人々にテレコミュニケーションの「クラウド化」と見なされてきました。

5Gのセキュリティを強化するソフトウェア

クラウドベース・アーキテクチャ

- 高いレジリエンス
- スケーラブルなセキュリティ
- ダイナミックなレスポンス

仮想ネットワーク機能（VNF）

- カスタマイズされたセキュリティ・ソリューション
- 迅速な緩和（ミティゲーション）
- 多様で競争力のあるサプライチェーン

先進的なソフトウェアツール

- 人工知能（AI）主導のセキュリティ
- 頑強なネットワーク脅威監視
- 強力な暗号化とアイデンティティ管理

5Gネットワークは、旧世代の通信技術と根本的に異なっています。旧世代の通信ネットワークが陳腐化の早いハードウェアコンポーネントに依存してきたのに対し、5Gは、インターネット・プロトコル（IP）を用いてネットワーク機能を「仮想化する」ためにソフトウェアとクラウドのインフラを利用します。実際に、クラウドサービスは5Gにとって今後非常に重要となるため、5Gは多くの人々にテレコミュニケーションの「クラウド化」と見なされてきました。ネットワーク機能の仮想化とクラウド化は、ネットワークの管理とセキュリティに無数の新たな可能性を切り開くでしょう。例えば、ソフトウェアを軸としたSDN（Software-Defined Networking）を用いれば、特定環境の中で用いるデータと機器に合わせてカスタマイズされたセキュリティ管理を利用する、特別仕様の仮想環境を創り出すことができます。このようにネットワーク環境を個別にあつらえることにより、顧客のために高い作業効率を生み出すことが可能になり、セキュリティの強化とインフラの最新化に向けて再投資する人材と資金を確保することもできます。

こうした進歩のおかげで、5Gの導入によりサイバーセキュリティが大幅に向上する可能性が生まれます。レジリエントなクラウドベース・インフラと主要ネットワーク機能の仮想化を組み合わせることにより、従来よりもずっと広範なユーザー層を対象として、カスタマイズされた安全なネットワーク、スケーラブルなセキュリティ・ソリューション、および必須セキュリティ機能の標準化を実現することが可能になります。これらの利点はすなわち、5Gネットワークがサイバー防御の面で有利なスタートを切ることを示すものであり、政策立案者にはこういった進歩を活用する道が開かれることになるでしょう。

5Gに組み込まれたセキュリティの利点

- **スケーラブルなセキュリティ。**5Gネットワークはそのほとんどがソフトウェアベースであるため、ユーザーはオンデマンドのサービスとしての通信にアクセスし、セキュリティなどの機能を追加または削減することができるようになります。このようなモデルを使えば、ネットワークディフェンダーは脅威監視およびアナリティクスツールなどのセキュリティ資源を最も必要な場所に割り当てることもできます。

- **強化されたアイデンティティおよびデータ保護。**5Gネットワークには、個人ユーザーのトラッキングとスプーフィング（なりすまし）を防止し、アイデンティティ管理と認証を強化し、ユーザーの固有識別子などのデータ暗号化を拡大するプロトコルが組み込まれています。

- **カスタマイズされたセキュリティ・ソリューション。**5Gは、カスタマイズされたセキュリティ管理を備えたプライベート・ネットワーク、さまざまな種類の機器またはトラフィックに異なるルールを適用できるネットワーク・スライシング、および個々の機器に合わせたソフトウェアベースのセキュリティ更新を通して、個人および機器固有のニーズに取り組むためにカスタマイズされたセキュリティ・ソリューションを可能にします。

- **レジリエントなネットワーク。**5Gのクラウドベース・インフラは、物理的なハードウェアシステムに依存せず遠隔で仮想的にデータを保存するため、サーバーの広範なネットワークを活用します。このため、複数の物理的ロケーションにデータが保存され、サービスの停止は限定的となり、アジリティは高まり、サイバー攻撃の標的が取り除かれることになるため、レジリエンスを向上させることができます。

- **AIの力。**5Gのクラウドベース・インフラは、最先端の人工知能（AI）とデータ・アナリティクスツールを用いることで、ネットワークディフェンダーによる脅威の特定と悪意ある攻撃の阻止を容易にします。

5Gネットワークがもたらすデータフローと接続機器の比類なき増加に伴い、セキュリティのリスクが高まります。旧世代の通信技術に比べて送信データと分散型ネットワーク・アーキテクチャが急激に増加することにより、5Gネットワークは他の最先端技術の場合と同様に、悪意ある行為者に新たな機会をもたらします。次世代の通信技術を安全なものにするため、5Gのあらゆるレイヤーにセキュリティを構築する精力的な努力が必要です。

政府は、5G技術がもたらすセキュリティの利点を生かす機会を捉え、ますますつながりが広まる環境の中で生じる新たなセキュリティの課題に取り組まなければなりません。産業界にセキュリティ対策の優先順位付けを奨励し、新しいセキュリティ技術および方法の開発を促進するとともに、セキュリティに対する効果的で持続可能なアプローチについての国際的なコンセンサスを構築するなどの方策において、政府が重要な役割を担うことにより、5Gの可能性を解き放つことに貢献できます。効果的な5Gのセキュリティ政策によって、政府は5Gから経済とサイバーセキュリティの計り知れない恩恵を受けることが可能です。

政府は、5Gネットワークの信頼性とセキュリティの確立に向けて主導的な役割を果たすべきです。具体的に言えば、政府は**ソフトウェア・イノベーションの活用、5Gエコシステムの確立、クラウドの強化、サプライチェーンリスクの管理、スマートで効果的な5Gガバナンスの構築を行う必要**があります。

これらの優先事項は、政府と国民が5Gのもたらすセキュリティの恩恵を受けるために役立つでしょう。ただし、5Gネットワークは何もない状況下では成長しません。政府と産業界による5G技術の展開と確立の取組みを支えるのは、未来のサイバーセキュリティの課題に対応するための訓練を受けた、能力ある労働力です。BSAの「Policy Agenda to Build Tomorrow's Workforce（未来の労働力を構築するポリシーアジェンダ）」は、堅牢な5Gセキュリティの支援も含め、幅広い経済的、社会的イノベーションに不可欠な21世紀の労働力を構築するための優先事項について概説しています。

政府は、5G技術がもたらすセキュリティの利点を生かす機会を捉え、ますますつながりが広まる環境の中で生じる新たなセキュリティの課題に取り組まなければなりません。

安全な5Gに向けた優先事項

ソフトウェア・イノベーションの活用

5Gネットワークの基幹として、ソフトウェアベースの革新的なツールと技術が5Gネットワークの動作のみならず、安全性確立のかたちを根本的に変えるでしょう。5Gネットワークにはセキュリティの課題に対するソフトウェア・ソリューションが含まれており、政府はそのようなソリューションの導入を主導しなければなりません。具体的に、政府は以下を実行する必要があります。

» **主要ネットワーク機能を仮想化する有望な技術に投資する。**
無線アクセスネットワーク（RAN）などの重要な5Gネットワークノードにおけるハードウェアインフラは、サプライチェーンの危殆化、独自の標準などの問題によるセキュリティの課題を生み出す場合があります。政府はこれらの課題に対し、競争を引き出しネットワークエッジのセキュリティを高める可能性を有するOpen RAN（オープンな、すなわち独自仕様でないインターフェースを用いるRAN）および仮想RAN（ソフトウェアベースのプラットフォームでRAN機能を実装するV-RAN）技術などのソフトウェア・ソリューションの開発と迅速な展開に投資する必要があります。

» **サイバーセキュリティの強化にソフトウェア・イノベーションを活用する。**
ソフトウェアを軸としたSDN、安全なネットワーク・スライシング、およびネットワーク機能の仮想化（NFV）などのソフトウェアベースの技術は、サイバーリスクを低減する新たな機会をもたらします。政策立案者は、疑わしい通信を分離し、機密情報を保護し、ユーザーを認証し、その他の主要セキュリティニーズに取り組む新しいセキュリティ技術の開発にこれらの技術を利用するために、ガイダンスを策定し、研究開発（R&D）を支援し、有望なアプローチを先導する必要があります。

» **5Gの研究開発ではセキュリティを優先する。**

5Gサービスに対するユーザーの要求が高まるにつれて、政府は5Gの可能性の実現に役立つ技術と方法に対する投資に注力しなければなりません。このような投資で優先すべきはセキュリティです。R&Dの資金調達によって、安全なネットワーク・スライシング、自動脆弱性スクリーニング、AIアプリケーション、サプライチェーン管理ツールなどの有望な手法の開発と実証を支援することができます。

5Gエコシステムの確立

5Gネットワークを確立するには、5Gネットワークのインフラを確立するだけでなく、ネットワークにつながる機器の大規模かつダイナミックなエコシステムを確立することが必要です。こうしたエコシステムには、ソフトウェア・アプリケーション、AIエンジン、IoT機器、および絶えず新しいデータを生み出して送信するその他のシステムが含まれます。政府は、真のエンドツーエンド・サイバーセキュリティを備えて5Gネットワーク上で動くシステムの、安全な設計、配置、構成、および保守を奨励すべきです。具体的に、政府は以下を実行する必要があります。

» **安全なソフトウェアを奨励する。**

5Gはソフトウェアで動くため、ソフトウェア脆弱性のリスクを低減することが従来にも増して重要になります。このために政府は、ソフトウェアの開発者とベンダーによる安全なソフトウェアの開発および維持に役立つガイダンスとベストプラクティスを導入すべきです。「BSA Framework for Secure Software（安全なソフトウェアのBSAフレームワーク）」は、政府と産業界がこの目標を達成するためのロードマップです。信頼の基点（roots of trust）などのハードウェアの安全を確立するためにソフトウェア・セキュリティをベストプラクティスと統合し、5Gエコシステムの全体にわたってシームレスなセキュリティを確保する必要があります。

» **強力な暗号化を支援する。**

5G環境における重要なセキュリティ・ツールの中で最も重要なのは、ネットワークを通過する膨大なデータの機密性と完全性を維持するために不可欠な暗号化です。政府は、入手可能な最強の暗号化ツールをネットワークとアプリケーションが利用できるように尽力し、量子コンピューティングなどの新たな技術を取り入れて生じてくる、進化を続ける脅威やセキュリティの課題に遅れを取らないように、新世代の暗号化技術の開発に投資すべきです。

» **機械学習と人工知能を活用する。**

AIおよび類似技術は、膨大なデータセットの全体にわたる脅威の特定と隔離を可能にし、監視を自動化し、インシデントレスポンスを支援するなど、5Gネットワークの安全性確立に極めて重要な役割を果たします。政府は、AIシステムの教育に利用できるデータセットを構築し、安全で透明なAIシステムの開発を奨励し、AIを重視したR&Dに投資することにより、AIによる5Gセキュリティの強化を支援できます。BSAは、この分野の政策立案者にとって指針となる「Five Key Pillars for Responsible AI（責任あるAIの5本の柱）」の概説を示しています。

» **IoT機器を確立する。**

5G技術の変形的利用の中で最も強力なのは、何十億ものIoT機器にわたる膨大なM2M（マシンツーマシン）のインタラクションでしょう。政府は、機器メーカーに安全なIoT機器の設計と安全性の維持を奨励する政策を確立する必要があります。そしてその政策は、利用可能な国際的に認められた規格と産業界のベストプラクティスを踏まえたものとし、最善の成果を達成するためにリスクベースかつ結果重視のフレームワークを導入するものであるべきです。

5Gネットワークを確立するには、5Gネットワークのインフラを確立するだけでなく、ネットワークにつながる機器の大規模かつダイナミックなエコシステムを確立することが必要です。

» **多層防御を構築したゼロトラスト環境を創り出す。**

ゼロトラスト・アーキテクチャは、ネットワーク内のすべてのユーザーとデータが脅威となり得ることを前提に、サプライチェーンの混乱から内部攻撃まで多岐にわたる脅威を低減する柔軟な多層の防御を構築するものです。ゼロトラスト5G環境の構築には、ハードウェアとソフトウェアのシステムを可能な限り分離することの他に、堅牢なユーザー認証プロトコル、ユビキタス暗号化、および強力なオープンソース駆動型アーキテクチャが必要です。政府は規格の策定、ベストプラクティス指針、およびR&Dへの貢献を通じてゼロトラストのアプローチを推進することができます。

クラウドの強化

クラウドサービスは、中核的な運用サービスからエッジコンピューティング環境まで、5Gネットワーク・アーキテクチャの中心的役割を果たします。クラウドのインフラは、迅速な緩和（ミティゲーション）の展開、セキュリティとリソースの要求に合わせたコンピューティング資源のダイナミックな割り当て、およびネットワーク全体のレジリエンス強化を可能にすることも含め、5Gのセキュリティ上の利点を数多くもたらします。このような利点を十分に活用するには、安全で信頼できるクラウド環境が必要です。政府は以下を実行する必要があります。

クラウドのインフラは、5Gのセキュリティ上の利点を数多くもたらします。

» **リスクベースのクラウドセキュリティ政策を導入する。**

5Gネットワーク全体のセキュリティを確保するには、クラウド・プラットフォームの安全性確立を優先しなければなりません。それを効果的に行うために、政策はリスクベースとし、クラウドサービスが処理するさまざまな種類のデータと、それらのサービスがネットワーク内の位置に応じて提供する多様な機能で構成しなければなりません。ISO/IEC 27103規格や米国立標準技術研究所（NIST）の「Framework for Enhancing Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティを改善するためのフレームワーク）」などのリスクベースのアプローチは、プロバイダーが自身の置かれた特定の状況下で顧客とセキュリティのニーズに応えるために必要な柔軟性と適応性を維持しつつ、確実に最善のセキュリティ成果をもたらします。

» **クラウドセキュリティ政策を国際的に認められた規格に合わせる。**

国際標準化機構（ISO）の27000シリーズやSOC（Service Organization Controls/内部統制に関する国際認証）などの国際的に認められた規格は、クラウドセキュリティの保証と評価において明確かつ繰り返しが可能な基準を提供します。政府がクラウドセキュリティ政策をこれらの規格に合わせれば、プロバイダーは世界中のクラウド環境の安全を確立する一貫した基準を確保することができ、技術的な相互運用性を高めることができます。政府はさらに、クラウドサービスを最も信頼できるものにするベストプラクティスに対して、コンセンサスの得られた指針を反映させます。政府はまた、コンプライアンス活動の効率を最大限に高めるために、類似のセキュリティ要件を維持する他国との互恵協定の締結を検討する必要があります。

» **複雑なクラウド環境内の役割と責任を理解する。**

クラウドサービスが5Gネットワークおよびクラウドサービスが支える数多くのアプリケーションとサービスにとってより不可欠になるにつれて、クラウド環境はますます複雑でダイナミックなものになります。ベンダーは、組込みアイデンティティ管理や脅威監視サービスなど、顧客が自身のクラウド環境に組み込むさまざまなセキュリティサービスを提供します。クラウド環境への参加者が増えるにつれて、それぞれの参加者が責任を担うセキュリティとプライバシーの側面について混乱するリスクが生じます。例えば、クラウドのプロバイダーがある程度のセキュリティ管理策を組み入れ、その他の管理策を顧客に委ねる場合があります。顧客はこれらの管理策のいくつかを任せようと、組込みサービスプロバイダーと契約をするかもしれません。役割と責任についても、IaaS（Infrastructure-as-a-Service/サービスとしてのインフラ）やSaaS（Software-as-a-Service/サービスとしてのソフトウェア）など、クラウドサービスの種類によって異なる場合があります。クラウドセキュリティの評価に努めようとする政府は、こうした複雑な環境内の役割と責任を慎重に区別できる政策を確保しなければなりません。

サプライチェーンリスクの管理

5Gネットワークの安全性を確立するには、ネットワークのインフラを構成するハードウェアとソフトウェアについて戦略的選択を行う必要があります。効果的なサプライチェーンリスクマネジメントを実践することにより脆弱性が限定され、ディフェンダーによるネットワークの防御が容易になります。BSAは、2019年5月のプラハ5Gセキュリティ会議で採択された「プラハ提案（Prague Proposals）」を支持しています。これは、5G技術を非常に有望なものにしている諸々の利点をセキュリティが弱めることのないようにしながら、競争とイノベーションを同時に促進する方法でセキュリティ目標の達成を追究するように政府を導く提案です。具体的に、政府は以下を実行する必要があります。

» **サプライチェーンのセキュリティにリスクマネジメントのアプローチを導入する。**

リスクマネジメントには、起こりうる脅威、脆弱性、および潜在的影響の特定を通じたリスクの理解、リスクに合わせた緩和戦略の調整、ならびに最も関連があり潜在的な影響力のあるリスクに基づく優先順位付けが必要です。

» **政策の相互運用性を促進する。**

規制と技術規格に国境を越える一貫性と適合性があれば、国際協力が可能になり、イノベーションの混乱が避けられます。政策立案者は、技術が海外で開発されたというだけでその技術の取得や組込みを断定的に禁止することをせず、規格に基づくリスクマネジメントのフレームワークに従うべきです。

» **透明で公正なサプライチェーン政策を確保する。**

例外的状況がない限り、政府によるサプライチェーンマネジメント政策とその実行は、影響を受ける利害関係者への具体的な行動についての通知に加えて、国民に対して透明なものであるべきです。また、利害関係者が決定に対して要求または抗議する機会、申し立てられた違反を弁護する機会、あるいは過去の懸念を修復する機会を含め、紛争を解決するための有意義なメカニズムを確立する必要があります。紛争解決のメカニズムは、リスク低減に向けたツールを制限することなく必然性と予測可能性の環境を生み出します。

» **セキュリティの強化に向けて政府と産業界の協力を促進する。**

このような政策は、政府と産業界が情報を共有し、脅威を阻むために協力し、共有する課題に対する共通の解決策を見出すために協力して取り組めるようにするものであるべきです。政府はこれまでに、政府と産業界の共同タスクフォースの設立、マルチステークホルダー政策策定の取り組み、およびその他の共同フォーラムで成功を手にしています。そしてこれらのモデルはサプライチェーンの優先事項に取り組むために再現されるべきなのです。

» **サプライチェーン全体にわたってイノベーションと競争を推進する。**

政府の政策は、5Gについてのみならず、サプライチェーンのリスク管理に向けた技術的、手順的アプローチについてもイノベーションを奨励するものであるべきです。R&Dの取り組みは、特定されたシステミックリスクに対処する新たなアプローチの開発に的を絞るべきです。例えば、仮想化技術には無線アクセスネットワーク（RAN）の脆弱性に関連するシステミックリスクに対処できる可能性があります。また、サプライチェーンへの新規参入に対する障壁を減らすことは、健全でダイナミックなサプライヤー・エコシステムの実現に寄与します。

規制と技術基準に国境を越える一貫性と適合性があれば、国際協力が可能になり、イノベーションの混乱が避けられます。

スマートで効果的な5Gガバナンスの構築

強力なセキュリティ管理と技術的手段は、効果的な5Gガバナンス、とりわけ世界中の5G開発を支える技術標準に関する5Gガバナンスに依存しています。5Gガバナンスには国家間および国内のさまざまな政府機関の間の協力が必要です。5Gネットワークと支援技術の責任あるガバナンスに向けたメカニズムを確立するために、政府は以下を実行する必要があります。

» **ビルトイン・セキュリティを備えたオープン標準を導入する。**

オープン標準は相互運用性を促進し、実装における透明性と一貫性を保証し、一つのベンダーの技術が他のベンダーの技術と伝達し合えるようにします。これとは逆に、独自の標準は非公開な独自システムを支援します。相互運用性は、ネットワークトラフィックに対するネットワークオペレーターの可視性を確実に高め、多様なセキュリティ・ツールの選択肢を確実にユーザーにもたらすために不可欠です。最優先事項としてオープン標準にセキュリティを組み入れると、多様なネットワークの全体にわたり一貫したレベルの保護を維持することができます。安全なオープン標準を根付かせるために政府は、5Gネットワークが強固な基盤の上に確実に構築されるよう、規格開発をする組織とそのプロセスの支援および産業パートナーとの協力に投資しなければなりません。

» **信頼できるオープンソースのクラウドアーキテクチャを構築する。**

政府は、オープンソースのライセンシングとガバナンス体制の確立を支援し、オープンソースを支える規格を強く求めることにより、信頼できるオープンソース駆動型アーキテクチャのソリューションの開発を奨励すべきです。オープンソース駆動型アーキテクチャはイノベーションを加速し、コストを削減し、従来よりもオープンでダイナミックな市場を生み出すことができます。セキュリティの観点から見れば、このようなアプローチは、クリティカルなコードへの透明性と潜在的脆弱性を改善する可能性を有し、ハードウェアとソフトウェアのエコシステムを分離することによりサプライチェーン攻撃のリスクを低減できます。このような効用を実現するために政府は、オープンソース・ソリューションのセキュリティと信頼性に対する信用を強化する取り組みに投資する必要があります。

» **柔軟で協調的なガバナンス・メカニズムを確立する。**

5Gが多数のセクターにわたってますます重要になるにつれて、一貫性のない重複したガバナンスのリスクが生じています。それは通信セクター、交通セクター（自動走行車両の広範な導入を5Gが可能にする）、医療セクター（安全を最重視すべき医療機器を5Gが支援する）、金融セクター（オンライン金融取引を5Gが支える）などにおける重要な技術としての5Gに見受けられます。旧世代の通信ネットワークは通信サービスとして厳しく規制される場合があったのに対して、5Gは同時に多数の機能とクライアントにサービスを提供するクラウドサービスなどの中核インフラに依存しているので、通信に特有の規制にうまく適合しません。ガバナンスが成功するには、さまざまなセクターと機関にわたって統一された手法が必要です。そのようなガバナンスのメカニズムは、柔軟性があり、5Gネットワークに特有の利用方法と脅威にコンプライアンス要件を合わせるリスクベースの手法を構築するものでなければなりません。

5G技術には世界経済の有り様を変え、数十億人の生活の質を向上させるとともに、デジタルエコシステムを作り変え、人間の現実世界との関わり合い方に変化をもたらす可能性がありますが、ますますつながりが広まる環境の中で、5Gに伴う新たなセキュリティの課題が生じています。政府は、5G技術がもたらすセキュリティの利点を生かす機会を捉えて、経済とサイバーセキュリティの計り知れない恩恵を享受するべきです。